

# United States District Court

for the  
Western District of New York



United States of America

v.

Case No. 25-mj-5061  
(Filed Under Seal)

CROSS ABU COLE

*Defendant*

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about October 30, 2022, in the Western District of New York, and elsewhere, the defendant, **Cross COLE**, knowingly transmitted in interstate commerce, with the intent to extort money from another person, communications, that is, text messages containing threats to extort and injure reputation of Victim 1, a person known to the United States Attorney.

**All in violation of Title 18, United States Code, Section 875(d).**

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

*Complainant's signature*

BRYAN SCHEIBER  
SPECIAL AGENT  
FEDERAL BUREAU OF INVESTIGATION

*Printed name and title*

Sworn to and signed telephonically,

Date: April 1, 2025

*Judge's signature*

City and State: Buffalo, New York

HONORABLE MICHAEL J. ROEMER  
UNITED STATES MAGISTRATE JUDGE

*Printed name and title*

**AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT**

STATE OF NEW YORK                    )  
COUNTY OF ERIE                    )       SS:  
CITY OF BUFFALO                    )

I, Bryan Scheiber, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of a criminal complaint charging CROSS ABU COLE (hereinafter "COLE"), with a violation of Title 18, United States Code, Section 875(d) (Interstate Communications with Intent to Extort).

2. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since June 2021. I am currently assigned to the FBI Buffalo Field Office Cyber Task Force in Buffalo, New York, where I work on investigations relating to criminal and national security cyber intrusions. I received my bachelor's and master's degrees in computer science, have a Graduate Certificate in Computer Security and Information Assurance and hold several private sector computer security certifications. Prior to becoming an FBI Special Agent, I was a Computer Scientist with the FBI's Washington Field Office. My work in the FBI, as well as the training I have received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against the United States.

3. The facts set forth are based upon my personal observations, my training and experience, and information obtained during the course of the investigation from other members of law enforcement, involving the review of records, interviews of witnesses, and information and reports provided. Because this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a Criminal Complaint and Arrest Warrant, I have not included each and every fact known by the government for this investigation.

#### **PROBABLE CAUSE**

4. On October 30, 2022, VICTIM 1, a resident of Buffalo, New York, reported to the Federal Bureau of Investigation (“FBI”) that he was the victim in an extortion threat that involved the use of nude photographs of VICTIM 1 from when VICTIM 1 was a minor. VICTIM 1, at the time of his complaint, was an adult.

5. On November 2, 2022, FBI Agents interviewed VICTIM 1, who stated that on October 30, 2022, he received text messages from telephone number (440) 941-06XX (“SUBJECT TELEPHONE”) that demanded he send \$200 to the CashApp account “\$zettsa” otherwise VICTIM 1’s nude photographs would be sent to his Snapchat contacts.<sup>1</sup> VICTIM 1 then received two nude photographs of VICTIM 1 from when VICTIM 1 was a minor, one nude photograph of VICTIM 1’s friend, which VICTIM 1 stated had come from his Snapchat

---

<sup>1</sup> VICTIM 1 provided the FBI with screenshots for some of the texts received from the SUBJECT TELEPHONE on November 2, 2022. The FBI later obtained a search warrant that included Google Voice text message content for the SUBJECT TELEPHONE and confirmed that the text messages were accurate.



account, and a screenshot of VICTIM 1's Snapchat contacts. VICTIM 1 sent \$200 to the CashApp account but cancelled the payment after speaking with his father. He then continued to receive multiple text messages from the same telephone number that threatened the release of the nude photographs. Further, VICTIM 1 told the FBI that his Yahoo email account was hacked on or about September 29, 2022, and that his Yahoo account was connected to his Snapchat account. VICTIM 1 later learned that some of his Snapchat contacts had received VICTIM 1's nude photographs from a separate Snapchat account.

6. VICTIM 1 provided the FBI with an export from his Snapchat account that included, but was not limited to, login history, search history and the friending activity for VICTIM 1's Snapchat account. FBI's review of the VICTIM 1's Snapchat data found the login history included access from an IP Address ("IP ADDRESS 1") on October 30, 2022, from an Apple iPhone 13 located in Washington, D.C. VICTIM 1 advised he did not travel outside the Buffalo, New York, area during this period.

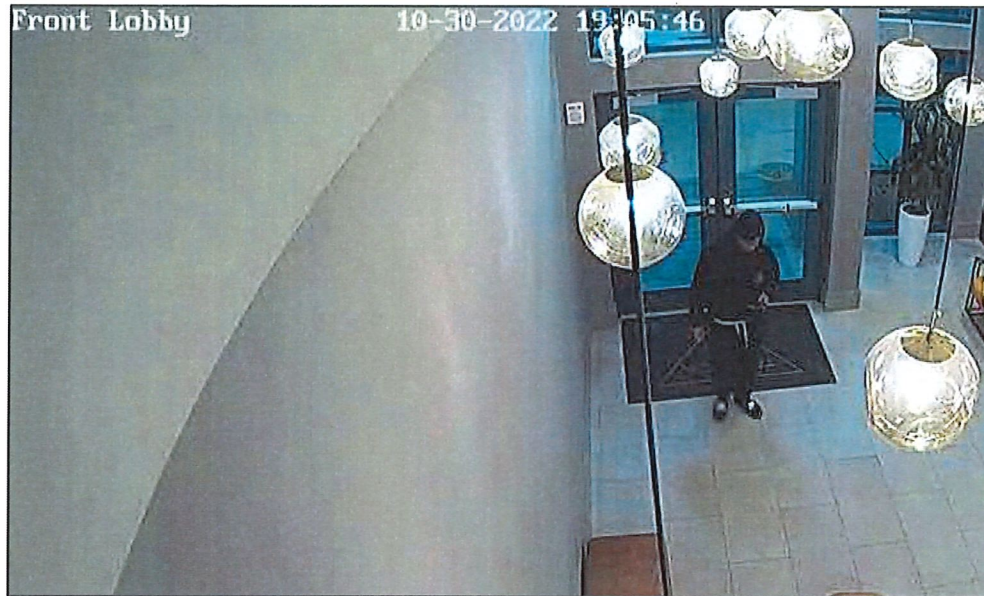
7. Law enforcement determined the SUBJECT TELEPHONE was a Google Voice telephone number subscribed to Google Account "CrossAmegashieD2@gmail.com" ("EMAIL ACCOUNT 1"). Google Voice is a telephone service that provides U.S. telephone numbers to Google Account customers. All Google Voice text communications travel through servers located outside of New York State. Google provided text message data for the SUBJECT TELEPHONE, which showed multiple outbound messages between the SUBJECT TELEPHONE and VICTIM 1's telephone number.

8. Google records for EMAIL ACCOUNT 1 listed the account owner as “Cross David” and showed that EMAIL ACCOUNT 1 was accessed from IP ADDRESS 1 on October 27, 2022 and from an additional IP Address (“IP ADDRESS 2”) on October 30, 2022.

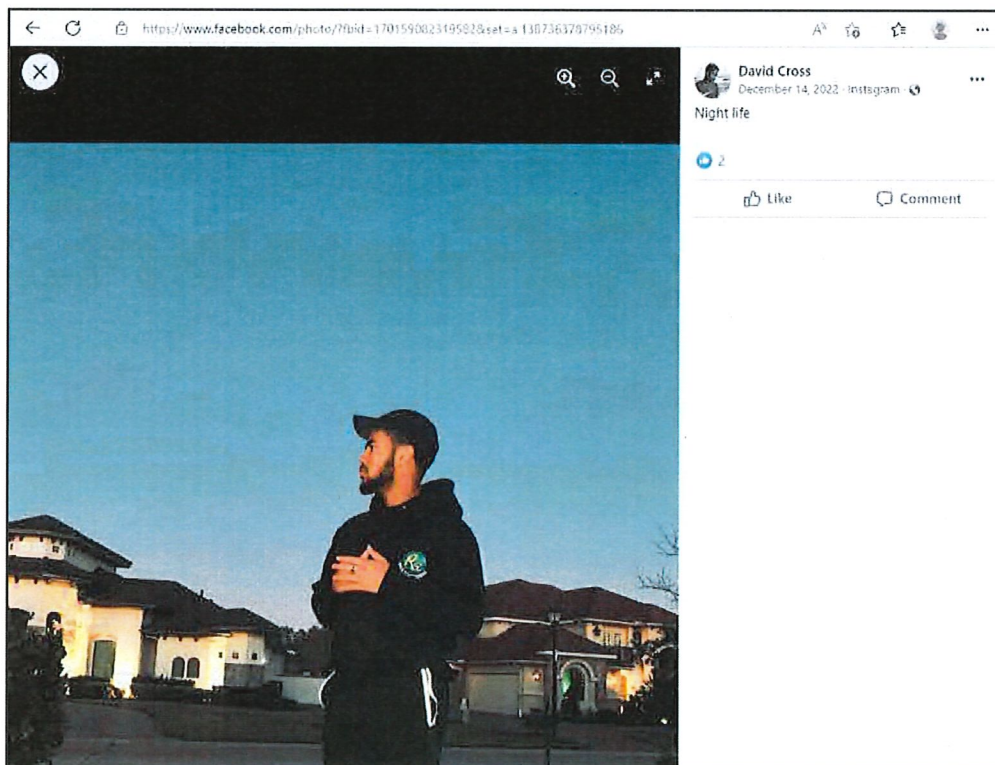
9. Verizon records for IP ADDRESS 1 listed the subscriber as the unit’s landlord with an address of 40 N ST NE UNIT 405 WASHINGTON, D.C. (“UNIT 405”). Records revealed, though, that the noted address was listed as an Airbnb rented to “VB”, an individual known to the affiant, during the relevant period, October 17, 2022, through November 7, 2022. Verizon records for IP ADDRESS 2 listed the subscriber as a business owned by VB with the same service address as IP ADDRESS 1.

10. Law enforcement identified VB as a Ghanaian citizen who entered the United States on October 18, 2022, with her son, CROSS ABU COLE (“COLE”) who was also a Ghanaian citizen.

11. Law enforcement obtained security camera footage for the apartment building that included UNIT 405, which showed an individual believed to be COLE entering the lobby on October 30, 2022, as shown in the security camera photo below.



12. Law enforcement located an open-sourced Facebook account, in the name “David Cross” that pictured an individual who matches COLE’s physical description and is wearing similar clothing to the surveillance footage.





13. Google records for EMAIL ACCOUNT 1, obtained with a federal search warrant, showed the account was accessed from IP ADDRESS 1 between October 19, 2022, and November 7, 2022 from devices that included an Apple iPhone 13. Additionally, emails within EMAIL ACCOUNT 1 included COLE's Ghanian university admissions application, multiple on-line product purchase emails that referenced the UNIT 405 Airbnb. Moreover, contained within the purchase orders was an Amazon.com receipt for "CROSS DAVID" that used UNIT 405 as the exact delivery address.

14. Law enforcement also located the threatening text messages and the nude photographs that were sent to VICTIM 1.

15. Law enforcement obtained a search warrant for an iCloud Account associated with EMAIL ACCOUNT 1. They located an iCloud note that included multiple Yahoo email addresses and passwords, including VICTIM 1's Yahoo email address, password and cellular telephone number. Thereafter, VICTIM 1 confirmed to the FBI that the password listed next to his Yahoo email address in the iCloud Note feature was, in fact, his Yahoo password.

16. The factual summary, including COLE's attempted extortion of \$200 in exchange for not releasing photos of VICTIM 1, was perpetuated using interstate communications, and establishes probable cause that COLE violated Title 18, United States Code, Section 875(d) (Interstate Threats).

CONCLUSION

17. I submit that there is probable cause to believe that COLE did violate Title 18, United States Code, Section 875(d)(Interstate Threats). Therefore, I request that the Court issue a criminal complaint and an arrest warrant, along with a sealing order.

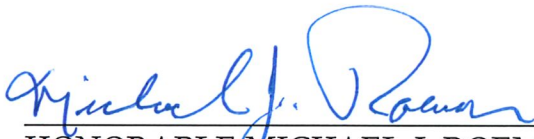
Respectfully submitted,



---

BRYAN SCHEIBER  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me  
Telephonically on April 1, 2025.



---

HONORABLE MICHAEL J. ROEMER  
United States Magistrate Judge